# **Security of Cyber-Physical Systems**

From Theory to Testbeds & Validation

#### Joaquin Garcia-Alfaro

CNRS SAMOVAR Lab & Télécom SudParis Université Paris-Saclay

CyberICPS, ESORICS 2016, September 27, 2016

## Context



http://www.panoptesec.eu/

#### Dynamic Risk Approaches for Automated Cyber Defense

FP7-ICT-2013-10



Context



http://www.panoptesec.eu/

Dynamic Risk Approaches for Automated Cyber Defense

FP7-ICT-2013-10



## What is SCADA?

#### • Supervisory Control And Data Acquisition

- Real-time technologies to centrally monitor/control remote/local equipment
- Distributed Control Systems E.g., large-scale transmission systems, such as electrical, oil and gas transportation networks



• Industrial Control Systems – Less degree of distribution, but synonym in this talk



## Motivation

- Malware moving from IT Systems to Operational Systems
- Wrong configurations, lack of encryption, legacy (vulnerable) systems, third party access, ...





#### **Proposed Methodology**

- Foster new theories,
- simulate/emulate case scenarios,
- & validate results using real environments.

# **Typical SCADA Elements (1/3)**

- **Probes/Sensors**: monitoring devices to retrieve measurements related to specific physical phenomena
- Effectors/Actuators: control devices, in charge of managing some external devices





# Typical SCADA Elements (2/3)

#### Middleware based on

- Remote Terminal Units
- Programmable Logic Controllers

to control those devices monitoring/controlling endpoints, often deployed far away from the backend





# **Typical SCADA Elements (3/3)**

IT/Master Terminal Units/Human Machine Interfaces

- Located at the control center of the organization
- Give access to the management of communications, collection of data, data storage, and control of sensors and actuators via the RTUs/PLCs







- ...

## **Security Challenges\***



#### Plus

- Reliability,
- Safety,
- Performance, ...

| Asset to protect: | Information                    | Process                       |  |
|-------------------|--------------------------------|-------------------------------|--|
| Priority          | IT Systems                     | MTUs to I/O                   |  |
| #1                | <u><b>C</b></u> onfidentiality | <u>A</u> vailability          |  |
| #2                | <u>Integrity</u>               | <u>Integrity</u>              |  |
| #3                | <u>A</u> vailability           | <b><u>C</u>onfidentiality</b> |  |

\* HIRSCHMANN, Why is Cyber Security Still a Problem? TOFINO Security Series



# The PANOPTESEC Approach

- Dynamic Risk Assessment
  - Preempt Exploitation of Vulnerabilities
  - Use of Attack & Operational ("Mission") Graphs



IT Security Oriented

**Operational Security Oriented** 



## **Project Emulation Environment** (1/10)

- Real control systems in cold standby mode (Disaster Recovery site)
- Real high/medium voltage substations in test mode
- Cloned SCADA systems for scalability emulation
- Simulated ICT domain for diversity of application experiments (e.g., non-SCADA environments)
- Installed network and security monitoring systems support data collection



acea

## **Project Emulation Environment (2/10)**



## **Project Emulation Environment (3/10)**

| a |          | LIN     |          | 1                 |      |         | C        |                              |    |
|---|----------|---------|----------|-------------------|------|---------|----------|------------------------------|----|
| U | <u> </u> | HV      |          |                   | п -  |         | C * 11 * |                              |    |
|   | ID       | Owner   | Group    | Name              | *    | Status  | Host     | IPs                          |    |
| - | 811      | rapone  | oneadmin | VR-02 (HV GPRS)   |      | RUNNING | esx02    | 10.10.0.150<br>192.168.1.201 | Ģ  |
|   | 777      | rapone  | oneadmin | TPT2K-HV-Virt-777 |      | RUNNING | esx02    | 172.21.100.159               | Ģ  |
|   | 776      | rapone  | oneadmin | TPT2K-HV-Virt-776 |      | RUNNING | esx02    | 172.21.100.158               | Ę. |
|   | 775      | rapone  | oneadmin | TPT2K-HV-Virt-775 |      | RUNNING | esx02    | 172.21.100.157               | Ģ  |
|   | 774      | rapone  | oneadmin | TPT2K-HV-Virt-774 |      | RUNNING | esx02    | 172.21.100.156               | 5  |
|   | 773      | rapone  | oneadmin | TPT2K-HV-Virt-773 | 2jíř | RUNNING | esx02    | 172.21.100.155               | Ģ  |
|   | 772      | rapone  | oneadmin | TPT2K-HV-Virt-772 |      | RUNNING | esx02    | 172.21.100.154               | Ģ  |
|   | 771      | rapone  | oneadmin | TPT2K-HV-Virt-771 |      | RUNNING | esx02    | 172.21.100.153               | Ģ  |
| 1 | 770      | Zidoune | oneadmin | TPT2K-HV-Virt-770 |      | RUNNING | esx02    | 172.21.100.152               | Ģ  |
|   | 769      | rapone  | oneadmin | TPT2K-HV-Virt-769 |      | RUNNING | esx02    | 172.21.100.151               | -  |
|   | 768      | rapone  | oneadmin | TPT2K-HV-Virt-768 |      | RUNNING | esx02    | 172.21.100.150               | ÷  |
|   | 767      | rapone  | oneadmin | TPT2K-HV-Virt-767 |      | RUNNING | esx02    | 172.21.100.149               | 9  |
|   | 766      | rapone  | oneadmin | TPT2K-HV-Virt-766 |      | RUNNING | esx02    | 172.21.100.148               | ÷  |
|   | 765      | rapone  | oneadmin | TPT2K-HV-Virt-765 |      | RUNNING | esx02    | 172.21.100.147               | -  |
|   | 764      | rapone  | oneadmin | TPT2K-HV-Virt-764 |      | RUNNING | esx02    | 172.21.100.146               | Ģ  |
| - | 763      | rapone  | oneadmin | TPT2K-HV-Virt-763 |      | RUNNING | esx02    | 172.21.100.145               | ÷  |
|   | 762      | rapone  | oneadmin | TPT2K-HV-Virt-762 |      | RUNNING | esx02    | 172.21.100.144               | -  |
| - | 761      | rapone  | oneadmin | TPT2K-HV-Virt-761 |      | RUNNING | esx02    | 172.21.100.143               | ÷  |
|   | 760      | rapone  | oneadmin | TPT2K-HV-Virt-760 |      | RUNNING | esx02    | 172.21.100.142               | -  |
|   | 759      | rapone  | oneadmin | TPT2K-HV-Virt-759 |      | RUNNING | esx02    | 172.21.100.141               | ÷  |
|   | 758      | rapone  | oneadmin | TPT2K-HV-Virt-758 |      | RUNNING | esx02    | 172.21.100.140               | ų, |

### **Project Emulation Environment (4/10)**

14:32:18.807376 ARP, Request who-has 172.21.100.197 tell 172.21.100.10, length 46 14:32:19.547769 ARP, Request who-has 172.21.100.232 tell 172.21.100.10, length 46 14:32:19.547809 ARP, Request who-has 172.21.100.209 tell 172.21.100.10, length 46 14:32:19.553328 ARP, Request who-has 172.21.100.169 tell 172.21.100.10, length 46 14:32:19.557392 ARP, Request who-has 172.21.100.236 tell 172.21.100.10, length 46 14:32:20.562219 ARP, Request who-has 172.21.100.199 tell 172.21.100.10, length 46 14:32:20.563395 ARP, Request who-has 172.21.100.237 tell 172.21.100.10, length 46 14:32:20.572426 ARP, Request who-has 172.21.100.238 tell 172.21.100.10, length 46 14:32:20.874248 IP 192.168.1.4 > 172.21.100.139: ICMP echo request, id 10512, seq 1, length 64 14:32:20.874290 IP 172.21.100.139 > 192.168.1.4: ICMP echo reply, id 10512, seg 1, length 64 14:32:20.876180 IP 192.168.1.4.60996 > 172.21.100.139.sumrpc: Flags [S], seg 2907222934, win 14600, options [mss 1460,sackOK,TS val 2761366341 ecr 0,mop,uscale 5], length 0 14:32:20.876238 IF 172.21.100.139.sumrpc > 192.168.1.4.60996: Flags [S.], seq 719133229, ack 2907222 935, win 28960, options Emss 1460,sackOK,TS val 488939676 eer 2761366341,nop,wscale 6], length 0 14:32:20.877093 IP 192.168.1.4.60996 > 172.21.100.139.sunrpc: Flags [.], ack 1, win 457, options [no p,nop,TS val 2761366341 ecr 4889396761, length 0 14:32:20.877154 IP 192.168.1.4.60996 > 172.21.100.139.sunrpc: Flags [P.], seg 1:61, ack 1, win 457, options [nop,nop,TS val 2761366341 ecr 4889396767, length 60 14:32:20.877170 IP 172.21.100.139.sumrpc > 192.168.1.4.60996: Flags [.], ack 61, win 453, options [n op,nop,TS val 488939677 ecr 27613663411, length 0 14:32:20.877833 IP 172.21.100.139.sunrpc > 192.168.1.4.60996: Flags [P.], seg 1:33, ack 61, win 453, options [nop,nop,TS val 488939677 ecr 2761366341], length 32 14:32:20.878647 IP 192.168.1.4.60996 > 172.21.100.139.sunrpc: Flags [.], ack 33, win 457, options [n op,nop,TS val 2761366342 ecr 4889396771, length 0 14:32:20.878664 IP 192.168.1.4.60996 > 172.21.100.139.sunrpc: Flags [F.], seg 61, ack 33, win 457, o ptions [nop.nop.TS val 2761366342 ecr 488939677], length 0 14:32:20.878781 IF 172.21.100.139.sunrpc > 192.168.1.4.60996: Flags [F.], seg 33, ack 62, win 453, c ptions [nop,nop,TS val 488939677 ecr 2761366342], length 0 14:32:20.888147 IP 192.168.1.4.60996 > 172.21.100.139.sunrpc: Flags [.], ack 34, win 457, options [n op,nop,TS val 2761366343 ecr 4889396771, length 0 14:32:21.553720 ARP, Request who-has 172.21.100.180 tell 172.21.100.10, length 46 14:32:21.554540 ARP, Request who-has 172.21.100.230 tell 172.21.100.10, length 46 14:32:21.554553 ARP, Request who-has 172.21.100.229 tell 172.21.100.10, length 46 14:32:21.554557 ARP, Request who-has 172.21.100.177 tell 172.21.100.10, length 46 14:32:22.547715 ARP, Request who-has 172.21.100.178 tell 172.21.100.10, length 46 14:32:23.534770 ARP, Request who-has 172.21.100.231 tell 172.21.100.10, length 46

### **Project Emulation Environment (5/10)**

|                   |                  |                        | guest@PsecIMT: ~                                  | <u>+ - □</u>                        |
|-------------------|------------------|------------------------|---|-------------------------------------|
| •                 |                  |                        | guest@PsecIMT: ~ 144x42                           |                                     |
| guest@PsecIMT:~\$ | tail -f /tmp/p   | roactiveRiskProfileDae | n.log   |                                     |
|                   |                  |                        |   |                                     |
| 2016 12 00 14.02. | 40 001000 001    | Poement A new file w   | added to the Felder containing the Preastive Pig  | k Profilos                          |
| 2010-12-09 14:03: | 51 267274 - DD   | P-Daemon: A new file w | he new Proactive Risk Profile to Security Policy  | K FIUILLES<br>Instantiation         |
| 2010-12-09 14:03: | 51.207274 - PR   | P-Daemon:> Fassing     | Security Policy Instantiation <                   |                                     |
| 2010-12-09 14.05. |                  |                        | Security Policy instantiation Contents            |                                     |
| >>> Loading neede | ed files!        |                        |   |                                     |
| Louding needs     |                  |                        |   |                                     |
| The file " /var/F | PANOPTESEC/Jail  | /InputData/MissionGrap | MissionGraph 12 08 2016 04 54 47.json " is a vali | d JSON File                         |
| The file " /var/F | PANOPTESEC/Jail  | /InputData/AttackGraph | ttackGraph 12 08 2016 04 54 47.json " is a valid  | JSON File                           |
| The file " /var/F | ANOPTESEC/Jail   | /InputData/AbstractDef | ltSecurityPolicy/ADSP-Minimal 2016-12-09 12-02-10 | -508384.json " is a valid JSON File |
| The file " /var/F | PANOPTESEC/Jail  | /InputData/AuthorizedM | igationActionList/EmulationEnvironmentAuthorizedM | IA V3.json " is a valid JSON File   |
|                   |                  |                        |   |                                     |
| >>> Adding to ROP | RI all the PEP i | in the Network Invento | for the current snapshot: 12/08/2016 04:54:47     |                                     |
|                   |                  |                        |   |                                     |
| The following PEF | P values were as | ssigned:               |   |                                     |
| Name              | Туре             | Assigned to Organiz    | ion AEV   |                                     |
| PEP2_SRVMSCADA    | SRVMSCADA        | AceaSim_Env            | 710000.0  |                                     |
| PEP2_WEBSCADA     | WEBSCADA         | AceaSim_Env            | 45000.0   |                                     |
| PEP2_SRVXSCADA    | SRVXSCADA        | AceaSim_Env            | 710000.0  |                                     |
| PEP2_FEXSCADA     | FEXSCADA         | AceaSim_Env            | 1320 <u>0</u> 00.0                                |                                     |
| PEP2_FTPSRV       | FTPSRV           | AceaSim_Env            | 3000.0  |                                     |
| PEP2_HMISCADA     | HMISCADA         | AceaSim_Env            | 80000.0   |                                     |
| PEP2_NTPSRV       | NTPSRV           | AceaSim_Env            | 2000.0  |                                     |
| PEP2_VRTX         | VRTX             | AceaSim_Env            | 206796.0  |                                     |
| PEP2_HMIREMOTE    | HMIREMOTE        | AceaSim_Env            | 0.0   |                                     |
| PEP2_USERPC       | USERPC           | AceaSim_Env            | 1000.0  |                                     |
| PEP2_GWMSCADA     | GWMSCADA         | AceaSim_Env            | 410532.0  |                                     |
| PEP2_GWXSCADA     | GWXSCADA         | AceaSim_Env            | 615800.0  |                                     |
| PEP2_FWDR         | FWDR             | AceaSim_Env            | 105000.0  |                                     |
| PEP2_FWCEDET      | FWCEDET          | AceaSim_Env            | 105000.0  |                                     |
| PEP2_MGMSRV       | MGMSRV           | AceaSim_Env            | 4.0   |                                     |
| PEP2_RTUSCADA     | RTUSCADA         | AceaSim_Env            | 2445663.0   |                                     |
| PEP2_FEMSCADA     | FEMSCADA         | AceaSim_Env            | 660000.0  |                                     |
| PEP2_VGR0UTER     | VGROUTER         | AceaSim_Env            | 27375.0   |                                     |
|                   |                  |                        |   |                                     |
|                   |                  |                        |   |                                     |
| >>> Compare Likel | lihood Values of | f Detrimental Events i | Proactive Risk Profile against Attack Scenario Th | reshold Values                      |
| *_*_*_*_*_*_*_*_* |                  |                        |   |                                     |
| Attack Sc         | cenario 'ASO1HV  | evaluation             |   |                                     |
| * * * * * * * *   | * * * * * * * *  | * * * * * * * * * * *  | * * *   |                                     |

### **Project Emulation Environment (6/10)**

|  | guest@PsecIMT: ~   | ◆ - ⊡ ×                               | 3 |
|--|--|---------------------------------------|---|
|  | guest@PsecIMT: ~ 157x42  |                                       |   |
| >>> Cc                                 | mpare Likelihood Values of Detrimental Events in Proactive Risk Profile against Attack Scenario Threshold Values | -                                     | • |
|  |  |                                       |   |
|  | Attack Scenario 'AS01HV' evaluation  |                                       |   |
|  |  |                                       |   |
| DE                                     | DE-BP-M-D ' likelihood: 1.0 Attack Scenario ' AS01HV ' threshold: 0.26   |                                       |   |
|  | DE Likelihood greater than Attack Scenario AS01HV threshold  |                                       |   |
|  | Collecting attack path IDs related to DE DE-BP-M-D   |                                       |   |
| DE                                     | DE-BP-M-C ' likelihood: 0.415 Attack Scenario ' AS01HV ' threshold: 0.26   |                                       |   |
|  | DE Likelihood greater than Attack Scenario ASOINV threshold  |                                       |   |
| >                                      | Collecting attack path IDs related to DE DE-BP-M-C   |                                       |   |
| DE                                     | DE-BP-H-C ' LIKeLIN00d: 0.415 Attack Scenario ' ASULHV ' threshold: 0.26   |                                       |   |
| ~                                      | DE LIKELINGOG Greater inan Attack Scenario ASGLAV infesnolo  |                                       |   |
| ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ | Collecting attack pain ibs related to be be-be-h-c   |                                       |   |
|  | DE-br-n-D Checkingou, 1.0 Actack Scenario AS01NV threshold   |                                       |   |
| Ś                                      | Collecting attack path Ths related to DF DF-RP-H-D   |                                       | 6 |
|  | concerning attack path ibs related to be be of the b   |                                       |   |
| >>> Cr                                 | eate Concrete Attack Vector for Threat 'AS01HV' with Attack Vector:  | · · · · · · · · · · · · · · · · · · · | ŧ |
| 'Entr                                  | vPoint=VGROUTER: Target1=WEBSCADA: \nTarget2=FTPSRV: BusinessDevice=FEXSCADA.SRVXSCADA'                          | -                                     | - |
| here                                   | is no Entry Point in the Mission Graph that matches the Attack Vector Entry Point!!!                             |                                       |   |
|  |  |                                       |   |
| >>> Fr                                 | om the information in Network Inventory the Concrete Attack Vector obtained is:                                  |                                       |   |
|  |  |                                       |   |
| >>> Ba                                 | ised on the information from Mission Graph the nodes in the Attack Vector for threat 'AS01HV' are:               |                                       |   |
| 0':                                    |  |                                       |   |
| 11:                                    | [u <sup>+</sup> _9fa408b-d9/9-4/94-9b6e-c004/8040856],   |                                       |   |
| . 5 . :                                | [u'e4/0DaaD-5088-4D20-aC28-blea42D5/0a3',  |                                       |   |
|  | u 3403/cou-bco-4/bi-dub0-/3240/(1404 ,   |                                       |   |
| 121.                                   | u / 180C323-90/0-4808-3029-01/014283/03 ],   |                                       |   |
|  | u b34b035d_116a.49b4-9052-353a0d15cad  |                                       |   |
|  | u 94/a1647-c1ac-4954-8a64-464f774ec99c'  |                                       |   |
|  | u'a21d2a42-0d63-4c78-a373-d45c7bc74cd3']}  |                                       |   |
| Intry                                  | Points:  |                                       |   |
|  | No nodes found!!   |                                       |   |
| arget                                  | : 1:   |                                       |   |
|  | c9fa4086-d979-4794-9b6e-cd0478040856 < STWEB   |                                       |   |
| arget                                  | 2:   |                                       |   |
|  | e470baab-5d88-4b20-ac28-61ea42b37da3 < FTPSRV01  |                                       |   |
|  | 94d37c8d-bc68-47bf-ad60-7524a77e1464 < ARCHIVESRV  |                                       |   |
|  | /18bC323-9d/8-4ada-9629-81/6t42a9/03 < dorete  |                                       |   |
| Busine                                 | ss Devices:  |                                       |   |
|  | d3480ddc-fe4a-4b94-9dc5-5cf94e658291 < mferp2  |                                       |   |
|  | 0540235d-116a-4904-9052-353a0d15caad < xterp1  |                                       |   |
|  | 04Ta1b4/-C1aC-4954-8ab4-4b4T//40C99C < XU0L1   |                                       |   |
|  | aziuza4z-0005-4C/8-a3/3-045C/DC/4C03 < XUELZ   |                                       |   |
|  |  |                                       |   |

### **Project Emulation Environment (7/10)**

| guest@PsecIMT: - 144x36           a21d2a42-0d63-4c78-a373-d45c7bc74cd3 < xuel2   |     | guest@PsecIMT: ~   | + _ D | × |
|--|-----|--|-------|---|
| a21d2ad2-0d63-4c78-a373-d45c7bc74cd3 < xuel2   |     | guest@PsecIMT: ~ 144x36  |       |   |
|  |     | a21d2a42-0d63-4c78-a373-d45c7bc74cd3 < xuel2   |       | ^ |
|  |     |  |       |   |
| <pre>&gt;&gt;&gt; The following nodes were seen in paths pointing to Business Devices:<br/>f2tb3rf5-ac2b-4221-8fa6-jhyyd65f663a &lt; TTY-T161<br/>c52e5ad7-6bc4-41db-bla2-2b7f8cd59lee &lt; TTY-T115-WU30<br/>d8a4e25a-d3ba-407e-9848-c5ceb6c687c &lt; TTY-T115-WU39<br/>l3cb5rce-2f67-451c-80d0-f3029adbbc1c TTY-T116-WU34<br/>b992e600-0de2-496c-ktK0-ssjenqaa123h7 &lt; mferp1<br/>ee07cace-9f56-4bcf-1935-a9d04f68c5 &lt; TTY-T116-WU32<br/>81629efd-9f20-1464d-b56f-29db612e72d4 &lt; TTY-T116-MU33<br/>10b2bble-9f23-4fe6-092e-1a26faf58e8 &lt; fegprs3<br/>75ccc10e-dc05-4529-a986-452f6ddbc9ba &lt; TTY-T115-MU28<br/>e470baa5-5888-4b20-ac28-610e42b37da3 &lt; FFP5RV01<br/>b54b235d-116a-49b4-9052-33530d15caad &lt; xferp1<br/>10b2bble-9f23-4fe8-092e-1a26/heaybd8 &lt; try-T115-MU28<br/>e6649d6d-6120-4c90-810-c093905b48 &lt; TTY-T115-MU28<br/>std7de-c414-4f09-a8da-1c60c0b88fc &lt; fegprs1<br/>718bc323-9d78-4ada-9629-8176f42a9708 &lt; dorete<br/>e6649d6d-6120-4c90-4310-c093905b48 &lt; TTY-T116-MU35<br/>876hhezq-77tq-4897-6659-j1hsfaqzs665 &lt; xferp2<br/>d3480dc-fe4a-4b49-9655-sc94be58291 &lt; ARCHIVESRV<br/>4d0343f-26e-445f-324a-96658291 &lt; TTY-T116-MU35<br/>876hhezq-77tq-4897-6659-j1hsfaqzs665 &lt; xferp2<br/>d3480dc-d794-9b6e-c0d786448656 &lt; STWEB<br/>469f4d55-ab61-484f-9454-hdqgz5776gv &lt; VR-T2<br/>11219477-723e-45d5-b4b2-9fdc730b865 &lt; STWEB<br/>469f4d55-ab61-484f-9454-hdqgz5776gv &lt; VR-T2<br/>11219477-723e-45d5-b4b2-9fdc730b8</pre> |     | Attack Graph Parsing   |       |   |
| <pre>&gt;&gt;&gt; The following nodes were seen in paths pointing to Business Devices:<br/>f2cb3cf5.ac2b.4221.8fa6.jhyyd65f663a &lt; TTY-T115.WV30<br/>d84425a.d3ba.407e.9848.c6cecb6c687c &lt; TTY-T115.WV30<br/>d84425a.d3ba.407e.9848.c6cecb6c687c &lt; TTY-T115.WV29<br/>l5cb5fcc.2f67.45L.e800e.f3029aadb8c1 &lt; TTY-T116.WV34<br/>b992e600.ede2.496c.kkk0.ssjenqaal23h7 &lt; mferp1<br/>ee07cace.9f56.4bcf.b835.a9d3db4f68c5 &lt; TTY-T116.WV32<br/>81629efd.9c91.464.db56f.29d04.c- TTY-T116.WV33<br/>19b2bb1e.9f23.4fe8.902e.la26feaf58e8 &lt; KALI<br/>aedda6d9.c3bf.4l62.93af.ef2639dc3c88 &lt; f6gprs3<br/>75cccl0e.dc05.4529.a986.452f6ddbc9ba &lt; TTY-T115.WV28<br/>e470baab.5d88.4b20.ac28.61ea42b37da3 &lt; FTPSRV01<br/>b54b235.116a.49b4.9952.ef35a30d15caad &lt; xferp1<br/>19b2bb1e.9f23.4fe8.902e.lajffeaf58e8 &lt; KALI2<br/>53a4d7de.c414.4f09.a8da.1c60c0bb7f &lt; f6gprs1<br/>71Bcc233.9d78.4ada.9629.8176f42a97d &lt; deprs1<br/>17bc233.9d78.4ada.9629.8176f42a97d &lt; deprs1<br/>17bc233.9d78.4ada.9629.8176f42a97d &lt; deprs1<br/>17bc233.9d78.4ada.9629.8176f42a97d &lt; deprs1<br/>17bc233.9d78.4ada.9629.8176f42a97d &lt; deprs1<br/>17bc233.9d78.4ada.9629.8176f42a97d &lt; acCHTVESRV<br/>4d0b343a.f2e0.445f.824a.806637443964 &lt; TTY-T116.WV35<br/>876hhezq.77tg.4897.6656.9j.jhsfaqzs665 &lt; xferp2<br/>cdfa4086.d979.4794.9dc5.ccf94c789b8c5 &lt; TTY-T116.WV31<br/>&gt;&gt;&gt; The PEP Type of the nodes that were seen in paths pointing to Business Devices are:<br/>FEXSCADA.VRTX, GWMSCADA, FTPSRV, WEBSCADA, MGMSRV, RTUSCADA</pre>  |     |  |       |   |
| f2cb3cf5.ac2b.4221.8fa6-jhyyd65f663a < TTY-T115.W30  | >>> | The following nodes were seen in paths pointing to Business Devices:   |       |   |
| cb2b3d7-bbc4-41db-bl2-2b7/8cd99lee < ITY-T115-MV30         d8a4e25a-d3ba-407e-9848-c5cecb5c687 < TTY-T115-MV30         b992e600-0de2-496c-kkk0-ssjenqaal23h7 < mferp1         ee07cace-9156-4hcf-b835-a9d0db4f68c5 < TTY-T116-MV32         8l629efd-9c91-464d-b5f-29d0b12e72d4 < TTY-T116-MV32         19b2bble-9f23-4fe8-902e-1a26feaf58e8 < KALI         aedda6d9-3bf-f120-39af-ef2639d3c388 < fegprs3         75ccc10e-dc05-4529-a986-452f6dbc9ba < TTY-T115-MV28         e470baab-5488-4b20-ac28-6iae42b37da3<         fe70baab-5488-4b20-ac28-6iae42b37da3<         ge70bab-5488-4b20-ac28-6iae42b37da3         fe70bab-5488-4b92-ac28-6iae42b37da3         ge70bab-5488-4b92-ac28-6iae42b37da3         ge70bab-5488-4b92-ac28-6iae42b37da3         ge70bab-5488-4b92-ac28-6iae42b37da3         ge70bab-5488-4b92-ac28-6iae42b37da3         ge70bab-5488-4b92-ac28-6iae42b37da3         ge70bab-5488-4b92-ac28-6iae42b37da3         ge70bab-5488-4b92-ac28-6iae42b37da3         ge70bab-6ix48-4b94-9052-353a0d15caad         ge70bab-1548-4b94-9052-353a0d15caad         ge70bab-1548-4b94-9052-353a0d15caad         ge70bab-1548-4b94-9052-353a0d15caad         ge70bab-1548-4b94-9052-353a0d15caad         ge70bab-16476-4494-9052-35437re14b4         ge70bab-16476-4494-962-9817-c- mferp2         g6436d-2612-4c94-3406-35-26194e58291   |     | f2cb3cf5-ac2b-4221-8fa6-jhyyd65f663a < TTY-T161  |       |   |
| d844223-3.03b-40/7e-9840-CbCeCbbC8/C < ITY-II15-WV29         15cb5fc=2f67-451:e300d-f3224a         b992e600-0de2-496c-kkk0-ssjenqaal23h7 < mferp1         ee07cace-9f56-4bcT-b835-a9d3db4f68c5 < TTY-II6-WV33         19b2bble-9f23-4fe8-902e-1a26feaf58e8 < KALI         aedda6d9-c3bf-4162-93af-ef2639dc3288 < fegprs3         75ccclbe-dc05-45276dbbcP32-d85fedbbc-extration         e470baab-5d88-4b20-ac28-61ea42b37da3 < FTPSRV01         b54235d-116a-49b4-9952-353a0d15caad < xferp1         19b2bb1e-9f23-4fe8-902e-1aj_jdheyyhd8 < KALI         S3a4d7de-c414-4f09-a8da-1c60c0bb87fc < fegprs1         71bbc323-9d78-4ada-9629-8176f42a9703 < dorete         e664940c2-6120-4c94-330-c39929305b48 < LANGUARD         94d37c8d-bc68-47bf-ad60-752437re1464 < ARCHIVESRV         4d0b343a-f2e0-445f-824a-806637443964 < TTY-116-WV35         876hberg-77tg-4897-655g-1156fa291 < mferp2         c9fa4086-d979-4794-9b6c-cd0478040856 < STWEB         469b463-5ab61-484f-9454-bfdc255 <<- STWEB         469fda5-3b61-484f-9454-bfdc255 <<-> TTY-116-WV31         >>>>       The PEP Type of the nodes that were seen in paths pointing to Business Devices are:         FEXSCADA, VRTX, GWMSCADA, FTPSRV, WEBSCADA, MGMSRV, RTUSCADA  |     | c62e5a0/-6bc4-41db-b1a2-2b/t8cd591ee < TTY-T115-MV30   |       |   |
| DSCB5TCE-2FD7-451C-8000-T3029aadb8C1 < TTY-T116-MV34         b9926600-0d2-4960-ckk0-sigenqaa1237< < mferp1         ee07cace-9f56-4bcf-b355-a9d3db4f68c5 < TTY-T116-MV32         81629efd-9c91-464d-b56f-23db612e72d4 < TTY-T116-MV32         1902b10=9f23-4fe8-902e-1a26feaf58e8 < KALI         aedda6d9-c3bf-4162-93af-ef2639dc3c88 < fepprs3         75cce10e-dc05-4529-a986-452f6ddbc9ba < TTY-T115-MV28         e470baab-5d88-4b20-ac28-61ead2b37da3 < FTP5RV01         b54b235d-116a-49b4-9952-353ad015caad < xferp1         19b2bb1e-9f23-4fe8-902e-1ajjdheyyhd8 < KALI2         53ad47dre-c414-4f09-a8da-1c60c0bb87fc < fegprs1         718b2323-9d78-4ada-9629-8176f42a9703 < dorete         e66496d2-6120-4c9d-a310-c039e398b48 < LANCUARD         94d37c8d-bc66-47bf-a660-7524a77e1464 < ARCHIVESRV         4d0b343a-f2e0-445f-824a-806637443964 < TTY-T116-MV35         876hberg-477tg-4897-665g-jisfsaqz6658         e0f496d2-6120-4c94-306-c52f94e658291 < mferp2         c9fa4086-d797-4794-906e-cd0478040856 < STWEB         496fd365-3b61-4k4f-9454-b4da9a57750y < VR-T2         11219477-723e-45d5-b4b2-9fdc730bb8c5 < TTY-T116-MV31  |     | 08a4e25a-03ba-40/e-9848-cbcecbbcb8/c < IIY-III5-MV29   |       |   |
| b992eb00-odc2-490C-KKR0-5Sjendal23h7 < mterp1         ee07cace-9f56-4b0C-Rb83-a9d3db4668C5 < TTY-T116-MV32         81629efd-9c91-464d-b56f-29db612e72d4 < TTY-T116-MV32         19b2bb1e-9f23-4fe8-902e-1a26feaf58e8 < KALI         aedda6d9-c3bf-4l62-93af-ef2639dc3288 < fegprs3         75cce10e-dc05-4529-a986-452f6dbbc9ba < TTY-T115-MV28         e470baab-5d88-4b20-ac28-61ea42b37da3 < FTPSRV01         b54b235d-116a-49b4-9652-353ad015cad < xferp1         19b2bb1e-9f23-4fe8-902e-1ajjdheyyhd8 < KALI2         S3a4d7de-c414-4f09-a8da-1c60e0bb87fc < fegprs1         718bc323-9d78-4da-9629-8176f42a973 < dorete         e06496d2-6120-4c9d-a310-cd93e9305b48 < LANGUARD         94d37c8d-bc68-47bf-adde-9629-8176f42a978         4d0b343a-f2e0-445f-824a-806637443964 < ARCHIVESRV         4d0b343a-f2e0-445f-824a-806637443964 < TTY-T116-MV35         876hhezq77tg-4897-6658:e1 <- xferp2         d3480ddc-fe4a-4b94-9dc5-5cf94e658291 < mferp2         c9fa4086-d979-4794-9b6c-cd0478040856 < STWEB         469fd355-ab61-484f-9454-bhdqaz5776gv < VR-T2         11219477-723e-45d5-b4b2-9fdc730bb8c5 < TTY-T116-MV31         >>> The PEP Type of the nodes that were seen in paths pointing to Business Devices are:         FEXSCADA,VRTX,GWMSCADA,FTPSRV,WEBSCADA,MGMSRV,RTUSCADA   |     | 15Cb5tce-2t6/-451C-8000-t3029aadb8c1 < TTY-T116-MV34   |       |   |
| BeeV/Cace-9750-40CT-0835-3903004766C5 < TTY-T116-MV32       I         81629efd-9c1-464-b56f-29db612e7d4 < TTY-T116-MV33       I         9b2bble-9f23-4fe8-902e-1a26feaf58e8 < KALI       I         aedda6d9-c3bf-4162-93af-ef2639dc3c88 < fegprs3       75cce10e-dc05-4529-a986-452f6ddbc9ba < TTY-T115-MV28         e470baab-5d88-db20-ac28-61ea42b37da3 < FTPSRV01       b54b235d-116a-49b4-9952-353a0d15caad < xferp1         19b2bb1e-9f23-4fe8-902e-1ajjdheyyhd8 < KALI2       S3ad47de-c414-4f99-a8da1-660c0b807fc < fegprs1         718bc323-9d78-4ada-9629-8176f42a9703 < dorete       e06496d2-6120-4c9d-a310-cd93e9305b48 < LANGUARD         94d37c8d-bc68-47bf-ad60-7524a77e1464 < ARCHIVESRV       4d0b343a-f2e0-445f-824a-806637443964 < TTY-T116-MV35         876hhezq-77tg-4897-665g-jjhsfaqzs665 < xferp2       c9fa4886-d079-4794-9b6e-cd0478040865 < STWEB         469fda55-ab61-484f-9454-hhdqazs776gv < VR-T2       11219477-723e-45d5-b4b2-9fdc730bb8c5 < TTY-T116-MV31         >>>> The PEP Type of the nodes that were seen in paths pointing to Business Devices are:       FEXSCADA, VRTX, GWMSCADA, FTPSRV, WEBSCADA, MGMSRV, RTUSCADA   |     | D992eb00-00e2-496C-KK0-s5jendaal230/ < mterpi  |       |   |
| abc/Serd-JcS1-4040-DSC1-29000120/204 < TTY-TIB-HV33       I         lpb2bble-9f23-4fc8-902c-la26fcafSe8 < KALI       regprs3         75cccl0e-dc05-4529-a986-452f6ddbc9ba < TTY-TIJ5-HV28       e470bbab-5d88-452 f6dab29rd3<         e470bbab-5d88-4526-ac28-6lea42b37d33 < FTPSRV01       b54b235d-116a-49b4-9052-353a0d15cad < xferp1         19b2bble-9f23-4fc8-902c-1ajjdheyyhd8 < KALIZ       S3a4d7dc-c414-4f09-a8da-1c60c0bb87fc < fegprs1         718bc323-9d78-4ada-9629-8176f42a9703 < dorete       e06496d2-6120-4c9d-a310-cd93e9305b48 < LANGUARD         94d37c8d-bc68-47bf-ad60-7524a77e1464 < ARCHIVESRV       4d0b343-f2e0-445f-824a-806637443964 < TTY-TITO-HV35         876hhezq-77tg-4897-665g-jjhsfaqzs665 < xferp2       d3480ddc-fe4a-4b94-9dc5-5cf94e658291 < mferp2         c9fad86-d979-4794-9b6c-cd0478048056 < VR-T2       11219477-723e-45d5-b4b2-9fdc730bb8c5 < VR-T2         11219477-723e-45d5-b4b2-9fdc730bb8c5 < TTY-T116-MV31       >>> The PEP Type of the nodes that were seen in paths pointing to Business Devices are: FEXSCADA, VRTX, GWMSCADA, FTPSRV, WEBSCADA, MGMSRV, RTUSCADA  |     | eeu/cace-ytsb-4bct-b835-ayd3db4tb8C5 < IIY-IIIb-MV32   |       |   |
| 19020010-9129-4168-9020-142010415068 < KALI         aedda69-c3bf-4162-93af.ef2639dc3288 < fepprs3         75cce10e-dc05-4529-a986-452f6ddbc9ba < TTY-T115-MV28         e470baab-5d88-420-ac28-61ea42b37da3 < FTP5RV01         b54b235d-116a-49b4-9052-353a0d15caad < xferp1         1902b1b-9f23-4fe8-902e-1ajjdheyhd8 < KALI2         53a4d7de-c414-4f09-a8da-1c60c0bb87fc < fegprs1         718bc323-9d78-4ada-9629-8176f42a9703 < dorete         e06496d2-6120-4c9d-a310-cd93e9305b48 < LANGUARD         94d37c8d-bc68-47bf-ad60-7524a77e1464 < ARCHIVESRV         4d0b343a-f2e0-445f-824a-806637443964 < TTY-T116-MV35         876hhezq-77tg-4897-665g-jjhsfaqze65         976404c-fe4a-4994-9dc5-5cf94e658291 < mferp2         c9fa4086-d979-4794-9b6e-cd0478040856 < STWEB         469fda55-ab61-484f-9454-hhdqazs776gv < VR-T2         11219477-723e-45d5-b4b2-9fdc730bb8c5 < TTY-T116-MV31   |     | 81029010-9091-4040-0007-129000120/204 < 111-1110-MV33  | Ţ     |   |
| abcdadors       14102-9341-01203000000 K       17141115-MV28         75cccel0e-dc05-4529-a986-45276d04050ba       TTY-T115-MV28         e470baab-5d88-4b20-ac28-61ea42b37da3       <>       FTPSRV01         b54b235d-116a-49b4-9952-353a0d15caad       <>       xferp1         19b2bb1e-9f23-4fe8-902e-1ajjdheyyhd8       <>       KALI2         53a4d7de-c414-4f09-a8da-1c60c0bb87fc       <>       fegprs1         718bc323-9d78-4ada-9629-8176f42a9703       <>       dorete         e06496d2-6120-4c9d-a310-cd93e9305b48       <>       LANGUARD         94d37c8d-bc68-47bf-ad60-7524a77e1464       <>       ARCHIVESRV         4d0b343a-f2e0-445f.824a-806637443964       <>       TTY-T116-MV35         876hherq-77tg-4897-6655c-jjhsfaqz565       <>       xferp2         d3480dc-fe4a-4b94-9dc5-5cf94e658291       <>       mferp2         c9fa4086-d979-4794-9b6e-cd0478040856       <->       STWEB         469fd355-ab61-484f-9454-hhdqazs776gv       <->       VR-T2         11219477-723e-45d5-b4b2-9fdc730bb8c5       <->       TTY-T116-MV31         >>>       The PEP Type of the nodes that were seen in paths pointing to Business Devices are:       FEXSCADA, VRTX, GWMSCADA, FTPSRV, WEBSCADA, MGMSRV, RTUSCADA  |     | 19020010-9123-4160-9020-142010415060 < NALI  |       |   |
| c470bab-5d88-4b20-ac28-6lea42b37da3 < FTPSRV01         b54b235d-116a-49b4-9052-353a0d15caad < xferp1         19b2bb1e-9f23-4fe8-902e-1ajjdheyyhd8 < KALI2         53a4d7de-c414-4f09-a8da-1c60c0bb87fc < fegprs1         718bc323-9d78-4daa-9629-8176f42a9703 < dorete         e06496d2-6120-4c9d-a310-cd93e9305b48 < LANGUARD         94d37c8d-bc68-47bf-ad60-7524a77e1464 < ARCHIVESRV         4d0b343a-f2e0-445f-824a-806637443964 < TTY-T116-MV35         876hbezq-77tg-4897-665g-jjhsfaqzs665 < xferp2         c9fa4086-d979-4794-9b6e-cd0478040856 < STWEB         469fda55-ab61-484f-9454-hhdqazs776gv < VR-T2         11219477-723e-45d5-b4b2-9fdc730bb8c5 < TTY-T116-MV31   |     | aeuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuu   |       |   |
| b47004a0-3008-4026-01247043       <  |     | /3CC2102-0C03-4329-0300-432100005904 < 111-1113-1420   |       |   |
| <pre>b34b25b1e-9f23-4fe8-902e-1ajjdheyyhd8 &lt; KALI2 19b2bb1e-9f23-4fe8-902e-1ajjdheyyhd8 &lt; KALI2 53a4d7de-c414-4f09-a8da-1c60c0bb87fc &lt; fegprs1 718bc323-9d78-4ada-9629-8176f42a9703 &lt; dorete e06496d2-6120-4c9d-a310-cd93e9305b48 &lt; LANGUARD 94d37c8d-bc68-47bf-ad60-7524a77e1464 &lt; ARCHIVESRV 4d0b343a-f2e0-445f-824a-806637443964 &lt; TTY-T116-MV35 876hhezq-77tg-4897-665g-jjhsfaqzs665 &lt; xferp2 d3480ddc-fe4a-4b94-9dc5-5cf94e658291 &lt; mferp2 c9fa4086-d979-4794-9b6e-cd0478040856 &lt; STWEB 469fda55-ab61-484f-9454-hhdqazs776gv &lt; VR-T2 11219477-723e-45d5-b4b2-9fdc730bb8c5 &lt; TTY-T116-MV31 &gt;&gt;&gt; The PEP Type of the nodes that were seen in paths pointing to Business Devices are: FEXSCADA, VRTX, GWMSCADA, FTPSRV, WEBSCADA, MGMSRV, RTUSCADA</pre>   |     |  |       |   |
| 1302001e=3123-4180-302e=14]jUneyNu8 < KAL12         53a4d7de-c414-4f09-a8da-1c60c0bb87fc < fegprs1         718bc323-9d78-4ada-9629-8176f42a9703 < dorete         e06496d2-6120-4c9d-a310-cd93e9305b48 < LANGUARD         94d37c8d-bc68-47bf-ad60-7524a77e1464 < ARCHIVESRV         4d0b343a-f2e0-445f-824a-806637443964 < TTY-T116-MV35         876hhezq-77tg-4897-665g-jjhsfaqzs665 < xferp2         c9f44086-d979-4794-9b6e-cd0478040856 < STWEB         469fda55-ab61-484f-9454-hhdqazs776gv < VR-T2         11219477-723e-45d5-b4b2-9fdc730bb8c5 < TTY-T116-MV31   |     | 1042530-1102-4504-5022-533001150a00 < XTELPI 1042540-4502 4650 0020 1351 dbauxbd9 < KALT2  |       |   |
| <pre>718bc323-9d78-4ada-9629-8176f42a9703 &lt; dorete<br/>e06496d2-6120-4c9d-a310-cd93e9305b48 &lt; LANGUARD<br/>94d37c8d-bc68-47bf-ad60-7524a77e1464 &lt; ARCHIVESRV<br/>4d0b343a-f2e0-445f-824a-806637443964 &lt; TTY-T116-MV35<br/>876hhezq-77tg-4897-665g-jjhsfaqzs665 &lt; xferp2<br/>d3480ddc-fe4a-4b94-9dc5-5cf94e658291 &lt; mferp2<br/>c9fa4086-d979-4794-9b6e-cd0478040856 &lt; STWEB<br/>469fda55-ab61-484f-9454-hhdqazs776gv &lt; VR-T2<br/>11219477-723e-45d5-b4b2-9fdc730bb8c5 &lt; TTY-T116-MV31<br/>&gt;&gt;&gt; The PEP Type of the nodes that were seen in paths pointing to Business Devices are:<br/>FEXSCADA, VRTX, GWMSCADA, FTPSRV, WEBSCADA, MGMSRV, RTUSCADA</pre>  |     | 15020012 + 9125 + 912 |       |   |
| <pre>e06496d2-6120-4c9d-a310-cd93e9305b48 &lt; LANGUARD 94d37c8d-bc68-47bf-ad60-7524a77e1464 &lt; ARCHIVESRV 4d0b343a-f2e0-445f-824a-806637443964 &lt; TTY-T116-MV35 876hhezq-77tg-4897-665g-jjhsfaqzs665 &lt; xferp2 d3480ddc-fe4a-4b94-9dc5-5cf94e658291 &lt; mferp2 c9fa4086-d979-4794-9b6e-cd0478040856 &lt; STWEB 469fda55-ab61-484f-9454-hhdqazs776gv &lt; VR-T2 11219477-723e-45d5-b4b2-9fdc730bb8c5 &lt; TTY-T116-MV31 &gt;&gt;&gt; The PEP Type of the nodes that were seen in paths pointing to Business Devices are: FEXSCADA, VRTX, GWMSCADA, FTPSRV, WEBSCADA, MGMSRV, RTUSCADA</pre>   |     | 718bc323.0d78-4da-0620.8176fd320703 < Tegpisi  |       |   |
| 94d37c8d-bc8a-d7bf-ad60-7524a77e1464 < ARCHIVESRV<br>4d0b343a-f2e0-445f-824a-806637443964 < TTY-T116-MV35<br>876hhezq-77tg-4897-665g-jjhsfaqzs665 < xferp2<br>d3480ddc-fe4a-4b94-9dc5-5cf94e658291 < mferp2<br>c9fa4086-d979-4794-9b6e-cd0478040856 < STWEB<br>469fda55-ab61-484f-9454-hhdqazs776gv < VR-T2<br>11219477-723e-45d5-b4b2-9fdc730bb8c5 < TTY-T116-MV31<br>>>> The PEP Type of the nodes that were seen in paths pointing to Business Devices are:<br>FEXSCADA, VRTX, GWMSCADA, FTPSRV, WEBSCADA, MGMSRV, RTUSCADA   |     | AB64962-6120-4-04-310-c40290235548 < 401612  |       |   |
| 4d0b343a-f2e0-445f-824a-806637443964 < TTY-T116-MV35<br>876hhezq-77tg-4897-665g-jjhsfaqzs665 < xferp2<br>d3480ddc-fe4a-4b94-9dc5-5cf94e658291 < mferp2<br>c9fa4086-d979-4794-9b6e-cd0478040856 < STWEB<br>469fda55-ab61-484f-9454-hhdqazs776gv < VR-T2<br>11219477-723e-45d5-b4b2-9fdc730bb8c5 < TTY-T116-MV31<br>>>> The PEP Type of the nodes that were seen in paths pointing to Business Devices are:<br>FEXSCADA, VRTX, GWMSCADA, FTPSRV, WEBSCADA, MGMSRV, RTUSCADA  |     |  |       |   |
| <pre>876bhezq-77tg-4897-665g-jjhsfaqzs665 &lt; xferp2<br/>d3480ddc-fe4a-4b94-9dc5-5cf94e658291 &lt; mferp2<br/>c9fa4086-d979-4794-9b6e-cd0478040856 &lt; STWEB<br/>469fda55-ab61-484f-9454-hhdqazs776gv &lt; VR-T2<br/>11219477-723e-45d5-b4b2-9fdc730bb8c5 &lt; TTY-T116-MV31<br/>&gt;&gt;&gt; The PEP Type of the nodes that were seen in paths pointing to Business Devices are:<br/>FEXSCADA,VRTX,GWMSCADA,FTPSRV,WEBSCADA,MGMSRV,RTUSCADA</pre>   |     | 4db343a_f2e0-445f_824a_806637443964 < TTY-T116_MV35  |       |   |
| d3480ddc-fe4a-4b94-9dc5-5cf94e658291 < mferp2<br>c9fa4086-d979-4794-9b6e-cd0478040856 < STWEB<br>469fda55-ab61-484f-9454-hhdqazs776gv < VR-T2<br>11219477-723e-45d5-b4b2-9fdc730bb8c5 < TTY-T116-MV31<br>>>> The PEP Type of the nodes that were seen in paths pointing to Business Devices are:<br>FEXSCADA,VRTX,GWMSCADA,FTPSRV,WEBSCADA,MGMSRV,RTUSCADA   |     | 376hbczn = 777cn = 4897 - 665n - i i hsfanzs65 <   |       |   |
| c9fa4086-d979-4794-9b6e-cd0478040856 < STWEB<br>469fda55-ab61-484f-9454-hhdqazs776gv < VR-T2<br>11219477-723e-45d5-b4b2-9fdc730bb8c5 < TTY-T116-MV31<br>>>> The PEP Type of the nodes that were seen in paths pointing to Business Devices are:<br>FEXSCADA,VRTX,GWMSCADA,FTPSRV,WEBSCADA,MGMSRV,RTUSCADA  |     | 3488040/4b94_9dc5_5(94e658291 <  |       |   |
| 469fda55-ab61-484f-9454-hhdqazs776gv < VR-T2<br>11219477-723e-45d5-b4b2-9fdc730bb8c5 < TTY-T116-MV31<br>>>> The PEP Type of the nodes that were seen in paths pointing to Business Devices are:<br>FEXSCADA,VRTX,GWMSCADA,FTPSRV,WEBSCADA,MGMSRV,RTUSCADA  |     | C9fa4086-d979-4794-9b6e-cd0478040856 < STWEB   |       |   |
| 11219477-723e-45d5-b4b2-9fdc730bb8c5 < TTY-T116-MV31<br>>>> The PEP Type of the nodes that were seen in paths pointing to Business Devices are:<br>FEXSCADA,VRTX,GWMSCADA,FTPSRV,WEBSCADA,MGMSRV,RTUSCADA  |     | d69fda55-ab61-484f-9454-bhdgaz5776gy < VB-T2   |       |   |
| >>> The PEP Type of the nodes that were seen in paths pointing to Business Devices are:<br>FEXSCADA,VRTX,GWMSCADA,FTPSRV,WEBSCADA,MGMSRV,RTUSCADA  |     | 11219477-723e-45d5-b4b2-9fdc730bb8c5 < TTY-T116-MV31   |       |   |
| FEXSCADA, VRTX, GWMSCADA, FTPSRV, WEBSCADA, MGMSRV, RTUSCADA   | >>> | The PEP Type of the nodes that were seen in paths pointing to Business Devices are:  |       |   |
|  |     | FEXSCADA, VRTX, GWMSCADA, FTPSRV, WEBSCADA, MGMSRV, RTUSCADA   |       |   |
|  |     |  |       |   |

## **Project Emulation Environment (8/10)**

| <b></b>   | guest@PsecIMT:   |  |               | ↑ _ □ ×  |
|---|--|--|---------------|----------|
| P   | guest@PsecIM   | Г: ~ 144x36                              |               |          |
|   |  |  |               | <b>▲</b> |
| >>>The following is the list of Mitig                   | gation Actions instantiated for threat:                        | AS01HV                                   |               |          |
| Name  | МА Туре  | PEP TYPE                                 | RM            |          |
| MA_AS01HV_FEXSCADA_ChangeHardware                       | MitigationActionChangeHardware                                 | FEXSCADA                                 | 2025.3164557  |          |
| MA_AS01HV_FEXSCADA_Reboot                               | MitigationActionReboot   | FEXSCADA                                 | 20.253164557  |          |
| MA_AS01HV_FEXSCADA_Patching                             | MitigationActionPatching                                       | FEXSCADA                                 | 2025.3164557  |          |
| MA_AS01HV_VRTX_ChangeHardware                           | MitigationActionChangeHardware                                 | VRTX                                     | 506.329113924 |          |
| MA_AS01HV_VRTX_Reboot                                   | MitigationActionReboot   | VRTX                                     | 5.06329113924 |          |
| MA_AS01HV_FTPSRV_Shutdown                               | MitigationActionShutdown                                       | FTPSRV                                   | 113.924050633 |          |
| MA_AS01HV_FTPSRV_Reboot                                 | MitigationActionReboot   | FTPSRV                                   | 7.59493670886 |          |
| MA_AS01HV_FTPSRV_Patching                               | MitigationActionPatching                                       | FTPSRV                                   | 759.493670886 |          |
| MA_AS01HV_WEBSCADA_Shutdown                             | MitigationActionShutdown                                       | WEBSCADA                                 | 56.9620253165 |          |
| MA_AS01HV_WEBSCADA_Reboot                               | MitigationActionReboot   | WEBSCADA                                 | 3.79746835443 |          |
| MA_AS01HV_WEBSCADA_Patching                             | MitigationActionPatching                                       | WEBSCADA                                 | 379.746835443 |          |
| MA_AS01HV_RTUSCADA_ChangeHardware                       | MitigationActionChangeHardware                                 | RTUSCADA                                 | 5696.20253165 |          |
| MA_AS01HV_RTUSCADA_Shutdown                             | MitigationActionShutdown                                       | RTUSCADA                                 | 854.430379747 |          |
| MA_AS01HV_RTUSCADA_Shutdown                             | MitigationActionShutdown                                       | RTUSCADA                                 | 854.430379747 |          |
| MA_AS01HV_RTUSCADA_Reboot                               | MitigationActionReboot   | RTUSCADA                                 | 56.9620253165 |          |
| MA_AS01HV_RTUSCADA_Patching                             | MitigationActionPatching                                       | RTUSCADA                                 | 5696.20253165 |          |
| Warning: The following PEPType don't<br>GWMSCADA,MGMSRV | have Authorized Mitigation Actions pre-                        | defined:                                 |               |          |
| >>>Concrete Values of Mitigation Act:                   | ions for: AS01HV   |  |               |          |
| > MA_AS01HV_RTUSCADA_ChangeHardwa                       | re   |  |               |          |
|   | f2cb3cf5-ac2b-4221-8fa6-jhyyd65f663a <                         | TTY-T161                                 |               |          |
| > MA_AS01HV_FEXSCADA_Reboot will                        | reboot the nodes:  |  |               |          |
|   | b54b235d - 116a - 49b4 - 9052<br>d3480ddc - fe4a - 4b94 - 9dc5 | -353a0d15caad < xf<br>-5cf94e658291 < mf | erp1<br>erp2  |          |
| > MA_AS01HV_VRTX_ChangeHardware                         |  |  |               |          |
| 46  | 9fda55-ab61-484f-9454-hhdqazs776gv < V                         | R-T2                                     |               |          |
| > MA_AS01HV_VRTX_Reboot will rebo                       | ot the nodes:  |  |               |          |
|   | 469fda55-ab61-484f-9454-hhd                                    | qazs776gv < VR-T2                        |               |          |
| > MA_AS01HV_WEBSCADA_Shutdown wil                       | l shutdown the nodes:  |  |               |          |
|   | c9fa4086-d979-4794-  | 9b6e-cd0478040856 <-                     | - STWEB       |          |

### **Project Emulation Environment (9/10)**

|      | guest@PsecIMT: ~  | ↑ _ ⊡ ×  |
|------|---|----------|
|      | guest@PsecIMT: ~ 157x42   |          |
| •>>C | oncrete Values of Mitigation Actions for: AS01HV  | <b>^</b> |
| >    | MA_AS01HV_RTUSCADA_ChangeHardware   |          |
|      | f2cb3cf5-ac2b-4221-8fa6-jhyyd65f663a < TTY-T161   |          |
| >    | MA_AS01HV_FEXSCADA_Reboot will reboot the nodes:  |          |
|      | b54b235d-116a-49b4-9052-353a0d15caad < xferp1   |          |
|      | d3480ddc-fe4a-4b94-9dc5-5cf94e658291 < mferp2   |          |
|      | MA_AS01HV_VRTX_ChangeHardware   |          |
|      | 469fda55-ab61-484f-9454-hhdqazs776gv < VR-T2  |          |
|      | MA_AS01HV_VRTX_Reboot will reboot the nodes:  |          |
|      | 469fda55-ab61-484f-9454-hhdqazs776gv < VR-T2  |          |
|      | MA_AS01HV_WEBSCADA_Shutdown will shutdown the nodes:  |          |
|      | c9fa4086-d979-4794-9b6e-cd0478040856 < STWEB  |          |
|      | MA_AS01HV_FTPSRV_Patching will patch the nodes:   |          |
|      | 718bc323-9d78-4ada-9629-8176f42a9703 < dorete, against CVE:CVE-2008-4250  |          |
|      | 718bc323-9d78-4ada-9629-8176f42a9703 < dorete, against CVE:CVE-2006-3439  |          |
|      | e470baab-5d88-4b20-ac28-6lea42b37da3 < FTPSRV01, against CVE:CVE-2004-2687  |          |
|      | 94d37c8d-bc68-47bf-ad60-7524a77e1464 < ARCHIVESRV, against CVE:CVE-2009-2687  |          |
|      | e470baab-5d88-4b20-ac28-61ea42b37da3 < FTPSRV01, against CVE:CVE-2010-2075  |          |
|      | 9403/C80-DC68-4/bf-ad60-/524a//e1464 < ARCHIVESRV, against CVE:CVE-2010-20/5  |          |
| >    | MA_ASUINV_RIUSCADA_Shutdown will shutdown the nodes:  |          |
|      | C6225307-05C4-4100-0132-20778C059162 < TYY-T115-MV30  |          |
|      |   |          |
|      | 13CU31CU-210/-431C-8000-13029aduu8CI < TTY-T110-11034   |          |
|      | 91670674 0c01 / 0635 - 490300410605 < TTY T116 MV22   |          |
|      | 75ccc10c dc05 4520 026 45216ddc0ba < TTY T15 M/20   |          |
|      |   |          |
|      | 40003436-1260-4431-6244-60005/443904 < TTY-T116-MV33  |          |
|      | MA ASAINV WERSCADA Patching will patch the nodes:   |          |
|      | $r_{a}$ About we because for the nodes. $c_{a}$ and |          |
|      | C9fa4086-d979-4794-9b6e-cd0478040856 < STMEB, against CVE-CVE-2006-3439   |          |
| >    | MA ASQ1HV RTUSCADA Patching will patch the nodes:   |          |
|      | c62e5ad7-6bc4-41db-b1a2-2b7f8cd591ee < TTY-T115-MV30, against CVE:CVE-2004-0185   |          |
|      | d8a4e25a-d3ba-407e-9848-c6cecb6c687c < TTY-T115-MV29, against CVE:CVE-2004-0185   |          |
|      | 15cb5fce-2f67-451c-80d0-f3029aadb8c1 < TTY-T116-MV34, against CVE:CVE-2004-0185   |          |
|      | ee07cace-9f56-4bcf-b835-a9d3db4f68c5 < TTY-T116-MV32, against CVE:CVE-2004-0185   |          |
|      | 81629efd-9c91-464d-b56f-29db612e72d4 < TTY-T116-MV33, against CVE:CVE-2004-0185   |          |
|      | 75cce10e-dc05-4529-a986-452f6ddbc9ba < TTY-T115-MV28, against CVE:CVE-2004-0185   |          |
|      | 4d0b343a-f2e0-445f-824a-806637443964 < TTY-T116-MV35, against CVE:CVE-2004-0185   |          |
|      | 11219477-723e-45d5-b4b2-9fdc730bb8c5 < TTY-T116-MV31, against CVE:CVE-2004-0185   |          |
|      | c62e5ad7-6bc4-41db-b1a2-2b7f8cd591ee < TTY-T115-MV30, against CVE:CVE-2003-1327   |          |
|      | d8a4e25a-d3ba-407e-9848-c6cecb6c687c < TTY-T115-MV29, against CVE:CVE-2003-1327   |          |
|      |   |          |

### **Project Emulation Environment** (10/10)

| guest@PsecIMT: ~   | + _ □ × |
|--|---------|
| guest@PsecIMT: ~ 144x41  |         |
| Checking Parameters Given<br>Performing RORI evaluation for:<br>'AS01HV' incident at the organization: 'AceaSim_Env'   | <u></u> |
| Individual Results EQUIPMENT ID RISK MITIGATION RORIID NAME EQUIPMENT ID RISK MITIGATION RORIMA_AS01HV_WEBSCADA_Shutdown  MA_AS01HV_WEBSCADA_Shutdown WEBSCADA   0.0057  1.52942MA_AS01HV_WEBSCADA_Reboot MA_AS01HV_WEBSCADA_Reboot WEBSCADA   0.0380 10.160842MA_AS01HV_WEBSCADA_Patching MA_AS01HV_WEBSCADA_Patching WEBSCADA   0.0380 10.160842MA_AS01HV_FEXSCADA_ChangeHardware MA_AS01HV_FEXSCADA_ChangeHardware FEXSCADA   0.2025 47.832309MA_AS01HV_FEXSCADA_Reboot WEBSCADA   0.0020 0.510124MA_AS01HV_FEXSCADA_ChangeHardware MA_AS01HV_FEXSCADA_Patching FEXSCADA   0.2025 54.258792MA_AS01HV_RTUSCADA_ChangeHardware RTUSCADA   0.5696 152.224635MA_AS01HV_RTUSCADA_ChangeHardware RTUSCADA   0.0057  1.52942MA_AS01HV_FTPSRV_Shutdown MA_AS01HV_FTPSRV_Shutdown FTPSRV   0.0114 3.060182MA_AS01HV_FTPSRV_Shutdown MA_AS01HV_FTPSRV_Patching FTPSRV   0.0088 0.213501MA_AS01HV_FTPSRV_Patching MA_AS01HV_RTUSCADA_Shutdown RTUSCADA   0.0854 22.933236MA_AS01HV_VRTX_ChangeHardware MA_AS01HV_RTX_ChangeHardware VRTX   0.0005 0.107395MA_AS01HV_WTX_Reboot MA_AS01HV_RTUSCADA_Patching RTUSCADA   0.506 13.065779MA_AS01HV_VRTX_Reboot MA_AS01HV_RTUSCADA_Patching RTUSCADA   0.506 152.868995 < Best RORI index |         |
| The selected combination criteria is to only combine the Mitigation Actions which RORI is over the RORI average<br>The individual RORI average is:',rori_avg<br>The following Mitigation Actions are over such average:<br>- MA_AS01HV_FEXSCADA_ChangeHardware - MA_AS01HV_FEXSCADA_Patching - MA_AS01HV_RTUSCADA_ChangeHardware - MA_AS01HV_RTUSCADA_Patching -   |         |
| Combined Results<br>Mitigation Actions  RM  RORI Index<br>[MA_AS01HV_RTUSCADA_Patching<br>MA_AS01HV_FEXSCADA_Patching] 0.6708  179.8242 < Best RORI index<br>[MA_AS01HV_FEXSCADA_Patching<br>MA_AS01HV_RTUSCADA_ChangeHardware] 0.6708  179.1118<br>[MA_AS01HV_RTUSCADA_Patching   |         |
| MA_AS01HV_FEXSCADA_ChangeHardware] 0.6708  168.1711<br>[MA_AS01HV_FEXSCADA_ChangeHardware<br>MA_AS01HV_RTUSCADA_ChangeHardware] 0.6708  167.5167   |         |
| 19 Response Plans were generated for threat:AS01HV<br>Response Plans Saved in: /var/PANOPTESEC/RPGenerator/ResponsePlans/12-08-2016_04-54-47/AS01HV01HV_FTPSRV_Shutdown will shutdown the nodes  |         |

## **Evolution**

- Protect, as well, from threats that are affecting physical sensors and actuators
  - In other words ...



Source: Hacking Chemical Plants for Competition and Extortion, Krotofil and Larsen, DefCon23, 2015. 21

## **Physical Elements**

- **Probes/Sensors**: monitoring devices in to retrieve measurements related to specific physical phenomena
- Effectors/Actuators: control devices, in charge of managing some external devices





# **Physical Elements**

Middleware based on:

- Remote Terminal Units
- Programmable Logic Controllers

to control a myriad (thousand to million) of devices monitoring/controlling end-points, often deployed far away (hundreds to thousands of km) from the backend





# Outline

- Brief Introduction
- Cyber-Physical Systems
- Feedback Control Verification
- Summary & Perspectives

## **Fundamental Questions ...**

• What are Cyber-Physical Systems (CPSs)?

• Are CPSs new?

• How CPS security differs from traditional IT security?

## What are CPSs?

• Systems that monitor behavior of physical processes and *take actions to correct those behaviors* 

... but also

Another definition

"Systems with integrated computational and physical capabilities that **can interact with humans** through many new modalities"

## Are CPSs new?

#### Short answer: No, they are not\*



#### The Kommandogerät 40 (Anti-aircraft gun - World War II)

Integration of mechanics, electronics, communication
 Human(s) in the loop (required at least five humans to operate)

\* Cyber–Physical Systems: A Perspective at the Centennial. Kim and Kumar. Proceedings of the IEEE, Vol. 100, pages 1287-1308, May 2012.

# The key ingredient in a CPS: Control

- Control means making a (dynamical) system to work as required
- **Feedback** is used to compute a corrective **control action** based on the distance between a *reference signal* and the *system output*



• Examples: dynamically follow a trajectory (robotics), regulate a temperature, regulate the sending rate of a TCP sender (TCP cong. control), controlling a pendulum in its unstable equilibrium, etc.

## **Networked Control System**

• From a methodological standpoint, we can model a CPS using a Networked-Control System (NCS)

#### NCS definition

Control system whose control loops are connected through a communication network



## **Traditional Issues Studied in the NCS Literature**

- Stabilizing a system under network delays & packet losses
- Techniques to limit data rate (e.g., from control to plant)
- Energy efficient networking for Wireless NCS
- Security?
  - Since the *stuxnet* incident, the control community seems to be heavily working as well on security issues of CPSs

# **CPS Vulnerabilities**

- Traditional Security Issues at the Cyber layer
  - Unencrypted communications
  - Controller settings manually configured (remotely or in person)
  - Default usernames and passwords
  - ...
- Attack Surface
  - Physical & control (**Physical**-layer)
  - Communication & network (**Cyber**-layer)
  - Supervisory & management (Human-layer)
  - ...
- Attack Vectors
  - Data (Control & Measurements / Actuators & Sensors)
  - Estimations & **Orders** (Controller & HMIs)

- ...

## **Putting all Together ...**



**People & Control Loops** 



**Information and Communications** 

**Technologies (ICT)** 



**Networked Control System (NCS)** 



**Programmable Automata** 

**Sensors & Actuators** 

## **Sample Attacks\***



\* A secure control framework for resource-limited adversaries. Texeira et al., Automatica, 51(1):135-148, 2015.

## **Replay Attack**



- Step 1: Sensors output is recorded
- Step 2: Recorded sensors output is replayed and sent to the controller
- Step 3: A control signal is sent to disrupt system functionalities

## **Sample Attacks\***



\* A secure control framework for resource-limited adversaries. Texeira et al., Automatica, 51(1):135-148, 2015.

## **Prevention of CPS Attacks**

- A well-designed control system shall resist external disturbances (failures & attacks), to a certain degree
- Several control-theoretic techniques to prevent cyber-physical attacks have been proposed in the literature\*
- Most of the techniques aim at injecting authentication to the control signal & discover anomalous measurements
  - E.g., use a noisy control authentication signal to detect integrity attacks on sensor measurements
  - In the following, we elaborate further on the aforementioned technique

\* A survey on the security of cyber-physical systems. Wu, Sun, and Chen. Control Theory and Technology, 14(1):2–10, February 2016.

# Outline

- Brief Introduction
- Cyber-Physical Systems
- Feedback Control Verification
- Summary & Perspectives

# **Revisiting a Watermark-based Detection Scheme to Handle Cyber-Physical Attacks\***

Joint work with Jose Rubio-Hernan & Luca de Cicco

\* 11th International Conference on Availability, Reliability and Security (ARES 2016), August 2016. (Best Paper Runner-Up Award)

### The Mo et al. Approach\* (1/2)

System is modeled as follows:

$$x_{t+1} = Ax_t + Bu_t + w_t$$
$$y_t = Cx_t + v_t$$



\* Physical Authentication of Control Systems. Mo, Weerakkody and Sinopoli. IEEE Control Systems, Vol. 35, pages 93–109, 2015.

#### The Mo et al. Approach\* (2/2)

The control signal input of the plant is:

$$u_t = u_t^* + \Delta u_t$$

- $\Delta u \in \mathbb{R}^p$  are *p* Gaussian stationary processes independent from the noises
- A detector is used at the controller that computes alarms based on Kalman filter residues

$$g_t = \sum_{i=t-w+1}^{t} (y_i - C\hat{x}_{i|i-1})^T \mathcal{P}^{-1}(y_i - C\hat{x}_{i|i-1})$$
(1)

In normal operation (no attack)  $g_t$  is small

\* Physical Authentication of Control Systems. Mo, Weerakkody and Sinopoli. IEEE Control Systems, Vol. 35, pages 93–109, 2015.

#### Simulating the Approach in Matlab/Simulink



### Validating the Approach in Matlab/Simulink



#### A replay attack is started at time t = 700s

### **Uncovered Issues**

Via simulation, we can show that a cyber-physical adversary is able to escape the detector

#### Cyber-physical Adversary

An attacker that is able to eavesdrop the messages containing the output of the controller with the intention of improving its knowledge about the system model

- Such attacker can leverage system identification tools to gather the system model and extract the watermark  $\Delta u_t$  from  $u_t = u_t^* + \Delta u_t$
- The extracted watermark can be used to authenticate messages to disrupt system dynamics

## An Implementation of our Proposed Attack

- The attacker eavesdrops  $u_t$  and  $y_t$
- A Least Mean Square (LMS) filter is used to get an input-output model W from u<sub>t</sub> to y<sub>t</sub>
- By doing so the watermark  $\Delta u_t$  is obtained
- An arbitrary  $u'_t$  can be sent to the system
- We can extract  $y_t^*$  from  $y_t$  and record it
- We fake the controller by authenticating y<sup>\*</sup><sub>t</sub> with the acquired watermark

### Validating the Attack in Matlab/Simulink



A cyber-physical attack is started at time t = 700s

### **Detection Ratio**

To quantify the detector performance we use the **Detection Ratio (DR)** index:

$$DR = \frac{\sum_{t=T_0}^{T_0+T_a} \mathbf{1}_{g_t \ge \gamma}}{T_a} \in [0, 1]$$
(2)

- In words: amount of time an attack is detected (g<sub>t</sub> ≥ γ) divided by the attack duration T<sub>a</sub>
- DR = 0 if the attack is never detected, DR = 1 if it is always detected

#### **Comparing Cyber and Cyber-Physical Adversary DR**



The Watermark-Detector protection scheme by Mo et. al is not sufficiently robust against cyber-physical adversaries

#### **Revisiting the Mo et al. Approach**

Towards a multi-watermark cheme

Switch among N watermarks to increase the Detection Ratio

$$\Delta u_t = \Delta u_t^{(s(t,T))} \tag{3}$$

where  $\Delta u_t^{(i)}$  with  $i \in \mathcal{I} = 0, ..., N - 1$  is the *i*-th of the *N* watermarks, *T* is the periodicity and *T* is the switching period

We moved from a static watermark mechanism to an **adaptive** watermark mechanism

#### Three Watermarks, period T=20s



watermark

#### A Cyber-physical adversary which starts the attack at time t = 700s

49

#### **Three Watermarks, period T=7s**





- The attacker disrupt system dynamics (the controller does not perceive it)
- The attack is detected very quickly (DR higher wrt the previous case)
- High frequency oscillations in state dynamics due to the new watermark

#### **Detection Ration vs. Switching Frequency (CDF)**



## **Back to the Suggested Methodology**

- Malware moving from IT Systems to Operational Systems
- Wrong configurations, lack of encryption, legacy (vulnerable) systems, third party access, ...





#### **Proposed Methodology**

- Foster new theoretical models,
- simulate/emulate case scenarios,
- & validate results using some testbeds.

### **Preparing the Testbeds**



## **Sample Testbeds**





#### http://j.mp/TSPScada





## **Testbed** (*ongoing*) **Results**







## **Testbed** (*ongoing*) **Results**





|                 | Replay Attack | FIR Adaptive Attack<br>(Non-parametric Attack) | Parametric Attack |
|-----------------|---------------|--|-------------------|
| True Positives  | <b>35.94%</b> | 14.80%   | 11.37%            |
| False Negatives | 64.06%        | 85.20%   | 88.63%            |
| False Positives | 0.98%         | 1.66%  | 1.35%             |

# Outline

- Brief Introduction
- Cyber-Physical Systems
- Feedback Control Verification
- Summary & Perspectives

# Summary

- Challenging, multidisciplinary topic
  - Dynamic (networked-control) systems & analysis of large datasets
- Risk Assessment
  - Traditional IT-based methods may still be applicable
  - However, they cannot solve the problem completely
    - Fundamental differences between IT systems & CPSs
- Modeling, from a control-theoretic perspective, is a *must* 
  - Pay attention to adversary strategies from the attacker's angle
  - Assume attackers with knowledge about information systems & physical systems at the same time
  - Testbeds for the evaluation of emerging theories, methods & techniques
  - Use practical & real-time environments

# **Thank You. Questions?**

#### References

- Hirschmann. Why is Cyber Security Still a Problem? TOFINO Security Series, 2010.
- Kim & Kumar. Cyber–Physical Systems: A Perspective at the Centennial. *Proceedings of the IEEE*, Vol. 100, pages 1287-1308, May 2012.
- Krotofil & Larsen. Hacking Chemical Plants for Competition and Extortion, *DefCon23*, 2015.
- Texeira et al. A secure control framework for resource-limited adversaries. *Automatica*, 51(1):135-148, 2015.
- Wu, Sun & Chen. A survey on the security of cyber-physical systems. *Control Theory and Technology*, 14(1):2–10, February 2016.
- Rubio, De Cicco, & Garcia-Alfaro. Revisiting a Watermark-based Detection Scheme to Handle Cyber-Physical Attacks. *ARES 2016*, (*Best Paper Runner-Up Award*), August 2016.
- Mo, Weerakkody & Sinopoli. Physical Authentication of Control Systems. *IEEE Control Systems*, Vol. 35, pages 93–109, 2015.